CONFIDENTIAL

USPR

INPUT QUESTIONNAIRE

CATALOG. NO U S P R
SIC. CODE
SIZE CODE
AREA CODE
STUDY CODE
DATE MM DD YY

STUDY TITLE:

TYPE OF INTERVIEW: ☒ VENDOR ☐ TELEPHONE
☐ USER ☐ ON-SITE
☐ MAIL

INTERVIEWER: _____

COMPANY: _____ CO. TYPE: _____

ADDRESS: _____ SALES: _____

_____ # EMPL: _____

CITY: _____

STATE: _____ ZIP: _____

INDUSTRY ☐

☐ DISCRETE MANUFACTURING ☐ UTILITIES ☐ INSURANCE
☐ PROCESS MANUFACTURING ☐ RETAIL ☐ GOVERNMENT- FEDERAL
☐ TRANSPORTATION ☐ BANKING ☐ GOVERNMENT-STATE & LOCAL
☐ MEDICAL ☐ WHOLESALE ☐ EDUCATION
☐ SERVICES ☐ OTHER

INTERVIEWS

NAME TITLE TELEPHONE NO.

SUMMARY

REFERENCES

CATALOG NO. USPR

PROTECTING THE CORPORATE SOFTWARE INVESTMENT
VENDOR QUESTIONNAIRE

1. What products/services do you offer related to program/data security?

	Product Name	Number of Users	Price Range
1.			
2.			
3.			
4.			

2. What mainframe/mini operating systems do you support?

	IBM	Burroughs	Honeywell	DEC	H-P	Others
Mainframe/ Minis						
Operating Systems						

3. What are the levels of program/data security that your products provide?

- ☐ Personal _____
- ☐ Terminal _____
- ☐ Program _____
- ☐ File _____
- ☐ Data _____
- _____ _____
- _____ _____

4. How are audit trails provided?

_____

_____

_____

_____

5. How does the product provide for:

Multi-CPU Environment/Site

Multisite Environment

Distributed Environment

6. To what extent does the product/system provide for protecting the program/data by encryption?

☐ None ☐ DES ☐ Other

7. What modifications are necessary to incorporate the product into the operating system environment?

☐ None

☐

8. What is the overhead associated with the use of your product?

☐ System Efficiency: _____

_____

☐ User Access: _____

_____

9. What products do you offer in relation to program/data security for personal computers?

☐ None

	☐ IBM/PC (Compatible)	☐ Apple	☐ DEC	☐ Others
Product Name	_____	_____	_____	_____
Operating System	_____	_____	_____	_____
Users	_____	_____	_____	_____
Price Range	_____	_____	_____	_____

10. How is program/data security accomplished for personal computers?

☐ Hardware _____

_____

☐ Software _____

_____

☐ Disc _____

_____

☐ _____ _____

_____

11. Who (up to 3) are your major competitors?

		Mainframe/Mini	Micro
Vendor	1.		
	2.		
	3.		

12. What are the trends you see in providing program/data security?

☐ Hardware

☐ Software

☐ Market

PROJECT SPECIFICATION STATEMENT

A. Project Code: USPR B. Program ISP

C. Project Title PROTECTING THE CORPORATE SOFTWARE INVESTMENT

D. Objective: TO EVOLVE STRATEGIES FOR PROTECTING SOFTWARE developed in-house and acquired from loss or breach both in the mainframe and personal computer distributed environment

E. Audience (order of priority)

	User/ Vendor	Job Function	Type Company	Company Characteristics
1	User	MIS MGR	FORTUNE 1000	MANUFACTURING
2	USER	V.P. ADMINISTRATION	FORTUNE 1000	FINANCIAL
3				
4				
5				

F. Reasons for Choosing the Subject.

1. CLIENT INTEREST
2. CHANGING OPERATING ENVIRONMENT
3. HOT TOPIC
4.

G. Scope of Study

1. Includes: PROPRIETARY SOFTWARE
SYSTEMS SOFTWARE
IN-HOUSE
ACQUIRED

2. Excludes: HARDWARE AND SYSTEMS SECURITY

H. Uses of Report: PLANNING SOFTWARE SECURITY IN A DISTRIBUTED SYSTEMS ENVIRONMENT

I. Issues

1. How can software be designed to incorporate security protection?
2. What are the implications of software security in the distributed processing / office environment?
3. To what extent should management be involved in software security?
4. What Levels of security are available for software Products?
5. What are the costs to implement software security at each level?
6. To what extents should software be protected from physical disaster?
7. What are the trends in enhancing mainframe/micro software security?
8. What are the personal identification requirements for software security?
9. What is the impact of personal computer on software security?
10. What products and services are available to aid software security?

INPUT

J. Market Forecast [X] No [ ] Yes _____ Period

K. Delivery Modes Covered

- [ ] Remote Computing (RCS)
- [ ] Batch Processing
- [ ] Facilities Management
- [ ] Professional Services - Programming and Analysis
- [ ] Professional Services - Education and Consulting
- [ ] Integrated Systems
- [ ] _____
- [X] Systems Software - Mainframe/mini
- [X] Systems Software - Personal Computer
- [X] Application Software - Mainframe/mini
- [X] Applications Software - Personal Computer
- [ ] _____
- [ ] _____
- [ ] _____

L. Interview Profile

1. Type of Interview:

Type of Respondent	Type of Interview							
	On-Site		Phone		Mail		Total	
	Number	R/A or Senior	Number	R/A or Senior	Number	R/A or Senior	Number	R/A or Senior
User	0		0	0			0	0
Vendor	0		15	5			15	5
Other (Specify) _____								
Total	0		15	5			15	5

2. Respondent Characteristics

Number of Interviews	Job Function	Company Characteristics (e.g., SIC, Size, etc.)
8	Marketing Executive	$1-5M Software/hardware
7	Product Manager	$5-25M Software/hardware

M. Page Allocations

Text	46
Exhibits	7
Sub-total	53
Appendices	10
Total Pages	63

PROTECTING THE CORPORATE SOFTWARE INVESTMENT	# Exhibits	# Text	Total Pages
I. INTRODUCTION	0	2	(2)
A. Objective, Audience and Need	—		
B. Scope and Use	—		
C. Methodology	—		
D. Related INPUT Reports	—		
II. EXECUTIVE SUMMARY (Format = Standard)	2	6	(8)
A. Purpose	0	1	1
B. Findings	1	3	4
C. Recommendations	1	2	3
III. ASSESSING Software Security	1	8	(9)
A. ACCOUNTABILITY	1	2	
B. AUDITABILITY	0	2	
C. INTEGRITY	0	2	
D. USABILITY	0	2	
E.			
F.			
IV. ESTABLISHING a SOFTWARE SECURITY METHODOLOGY	2	12	(14)
A. IMPORTANCE OF PEOPLE	0	5	
B. OPTIONS	1	3	
C. SCOPE	1	4	
D.			
V. DESIGNING FOR SECURE SOFTWARE			
A. 1 ASSURANCE			
B. 2 INTEGRITY			
C. 3 AUDIT			
D.			
VI. The MICROcomputer and Software Security	0	8	(8)
A. Management	0	2	
B. Distributed Processing	0	5	
C. Software Storage	0	1	
D.			
VII. Vendor Product + Service	2	10	(12)
A. Software	2	8	
B. Hardware	0	2	
C.			
D.			
Sub-total Pages	7	46	(53)
APPENDIX VIII Conclusions & Recommendations	1	9	(10)
A. Definitions	0	5	
X B. Data Base			
C. RELATED INPUT REPORTS	1	0	
D.			
E. Questionnaire - Vendor	0	4	
X Questionnaire - User			
X Index			
Total Pages	8	55	(63)

Q. Other Research

1. Library: Source: ICP + DATA SOURCES

Objective: VENDOR REFERENCES

2. Reports:

Code	Title	Objective
ISP	NEW ISSUES IN COMPUTER SECURITY	

3. Other Sources:

VENDOR LITERATURE

P. Project Management

1. Project Manager: PAUL COLEN
2. Initiation Date: 5/31/84 Start Date: 6/4/84
3. Midpoint Review: 6/25/84
4. First Draft Due: 7/20/84
5. Word Processing Begin Date: 7/23/84
6. Shipping Date:

Q. Other Comments and Direction

R. Detailed Table of Contents Attached? Yes ____ No X

1984 QUARTERLY SCHEDULING PLAN (Q)

PROJECT: USPR

DATE: 6/1/84

PROJECT LEADER: PAUL COLEN

CORPORATE/WEEK ENDING

ACTIVITY / PROJECT	NAME	MAN DAYS	EFFICIENCY	ESMD	CORP WEEK END	JUNE 22 6/1	23 6/8	24 6/15	25 6/22	26 6/29	JULY 27 7/6	28 7/13	29 7/20	30 7/27
PROJECT (POLL) AUTHORIZATION/ SPECIFICATION	PC	1		1		6/1 ▽								
Q DESIGN	PC	1/2		1/2				6/15 ▽						
Q APPROVAL/ REVIEW MEETING		-		-										
INTERVIEWS ON SITE ( ) NO.														
INTERVIEWS PHONE (✓) NO. 15	PC	3		3				6/18 ▽ 1	1	6/25 ▽				
REVISED DATATAB AND ANALYSIS	PC	1		1 1/2						6/25 ▽ 6/29 ▽				
WRITING	PC	7		7							7/6 △	7	7/20 ▽	
ABSTRACT				-										
QC														
REPORT PROD. AND SHIPPING														
PRESENTATION														
"THANK YOU" MAILED														
PLAN				13		1	0	1 1/2	1	2 1/2	1	3	3	
ACTUAL														
CUM P/A														

INPUT

R12/83

6/4/84

Clients polled:

Ray Vasher	313-322-3020	Ford	6/1
Bernie Morse	818-714-2278	Litton	6/1
Bill Jatte	301-493-2139	Marriott	6/4
Ed Dudek	213-970-4779	Northrop	6/1
John Canter	412-434-3273	PPG Industries	6/1
Joe Zack	201-588-7809	Schering Plough	6/4
Donna Harris	813-224-3436	GTE Data Services	6/4

USPR

Client Pall

Stanley Garcynski	called 5/31 call back Thursday 6/4	American Hoechst	201-231-2020
James Anderson	called 5/31 to call back	6/1/84 call back Monday 6/4 Ashland Automation Serv. called 6/4	606-268-7682
Gail Lepard		Computer Sciences	213-615-0311
X Douglas Kilby:	6/1 Roy Washer 3020 Southmore	Ford	313-322-9396
L. E. Winship	DONNA HARRIS DAVE SALYER -3436 To call back	called 6/1 to call back GTE Data Services	called 6/4 to call back 813-224-3803
X Robert Huston -	to call back 818 716-2278 Bernie MORAR	6/1 will call back Litton Mellonics	818 -716-2237
X Arthur Hilley	BILL JAFFE 301-493-2139 To call back	Marriott called again 6/1/84 will call back called 6/4	301-897-1312
Kay Ames	ED KLERSY V.P. 313-256-5230	Mich. Consolidated Gas	313-256-5469
X Richard Lange	Phil Dr James - 213-970-2358 will call back	Northrop Corp. called 6/1 ED DUDEK-4779 213-970-4779 will call back	213-970-4938
Lori Campbell	called 5/31 to call back	Ohio Edison	216-384-5335
X John Canter	OK AS IS	PPG Industries	412-434-3273
Michael Studney	Joe BACK, 6/1/84 To call back	201-558-7907 6/4/84 called Schering Plough	201-558-4000
Keith Solheim	—	Soc. Security Admin.	301-594-9582
Joseph Cline	Bob Calegari called 5/31 To call back ~~Bob Calegary~~ X2014	called 6/1/84 to call back Southern New Eng. Tel. 203-771-2014 6/4	203-771-3134

USPR - Protecting Corporate Software Investment 15 ESHDs

- 6 Client interviews, regarding interest in subject (respecification phase)
- 15 Vendor interviews to be used in the report

Objective: Provide strategies for protecting software against destruction, loss, tampering, and theft. Develop guidelines for selecting security aids and the amount of protection that is required. Identify the implications of end-user software protection and the challenge of protecting software that is not resident in the corporate data center.

Topics to include:

- Available products
- Encryption
- Password Control } How effective, how much is too much,
- Key management } what makes it cost effective.
- The impact of PCs and end user computing on security

USPR

Client Pall

Stanley Garzynski	American Hoechst	201-231-2020
James Anderson	Ashland Automation Serv.	606-268-7682
Gail Leperd	Computer Sciences	213-615-0311
Douglas Kilby	Ford	313-322-9396
L. E. Winship	GTE Data Services	813-224-3803
Robert Huston	Litton Mellonics	213-716-2237
Arthur Helley	Marriott	301-897-1312
Kay Ames	Mich. Consolidated Gas	313-256-5469
Richard Lange	Northrop Corp.	213-970-4938
Lori Campbell	Ohio Edison	216-384-5335
John Carter	PPG Industries	412-434-3273
Michael Studney	Schering-Plough	201-558-4000
Keith Saltzein	Soc. Security Admin.	301-594-9582
Joseph Cline	Southern New Eng. Tel.	203-771-3134

Richard West Univ. of Cal. 415-642-2646

PROTECTING THE CORPORATE SYSTEMS AND SOFTWARE INVESTMENT

U-SPR BACKUP

U-SPR

PROTECTING THE CORPORATE SYSTEMS AND SOFTWARE INVESTMENT

CONTENTS

Page

I INTRODUCTION 1
- A. Background 1
- B. Scope and Methodology 2

II EXECUTIVE SUMMARY 5
- A. Establish a Baseline for Information Systems and Software Protection 6
- B. Security Protection Is a Three-Dimensional Assessment 8
- C. Layered Technology Is the Core Defense 10

III PEOPLE, THE KEY TO THE SYSTEM AND SOFTWARE SECURITY 13
- A. Security, a Top Management Responsibility 13
- B. A Well-Placed Security Director 15
- C. People Security Factors 17
  1. Background Investigation 17
  2. Employee Hiring Procedures 18
  3. Corporate Information Security Policy 18
  4. Employee Education 18
  5. Security Performance Evaluation 19
  6. Code of Conduct 19
  7. Separation of Duties 19
  8. Termination Procedures 21

IV ESTABLISHING A SOFTWARE SECURITY METHODOLOGY 23
- A. Software Security Administration 23
  1. Software Design and Development 23
  2. Documentation Control 23
  3. Fire Protection 24
  4. Disaster Recovery 24
  5. Legal 24
  6. Insurance 25
- B. Operational Software Security Options 25
  1. Passwords 25
  2. Terminal Identifier 29
  3. Security Monitors 29
  4. Encryption 31
  5. Telephone Access Controllers 32

6. Smart Cards 31
7. Other Technology 37

V DESIGNING FOR SECURE SOFTWARE 39
A. Systems Software 39
1. Operating Systems, the Key to Information Security 39
2. Data Base Management Systems, a Problem Area 43
B. Applications Software 46
1. Design 46
2. Programming 46
3. Validation 47
4. Maintenance 47

VI THE MICROCOMPUTER AND SOFTWARE SECURITY 49
A. Management 49
B. Distributed Processing 50
1. Encryption 51
2. Signatures 51
3. Fiber Optics 52
C. System and Software Security 52
1. Physical 52
2. Access Control 53
3. Secure Microprocessor 53
4. Secure Disk Storage 54

VII SUMMARY 59
A. People Count 61
B. Administration Necessary 62
C. Technology, the Core Defense 63

APPENDIX A: DEFINITIONS 65

APPENDIX B: RELATED INPUT REPORTS 71

APPENDIX C: VENDOR QUESTIONNAIRE 73

PROTECTING THE CORPORATE SYSTEMS AND SOFTWARE INVESTMENT

EXHIBITS

			Page
II	-1	Establish a Baseline for Information Systems and Software Protection	7
	-2	Security Protection Is a Three-Dimensional Assessment	9
	-3	Layered Technology Is the Core Defense	11
III	-1	Defense Against Possible Threats to Corporate Information Systems	14
	-2	Information Systems Code of Conduct	20
IV	-1	Levels of Security	26
	-2	Leading Security Monitors for IBM Plug-Compatible Systems	28
	-3	Telephone Access Controller Security System Interface	33
	-4	Smart Card Functional Design	36
V	-1	Implementation of Discretionary Security Policy	41
	-2	Secure Information Systems Execution Domains	42
	-3	Arbitration of User Queries to Protect DBMS Resources	45
VI	-1	Secure Microcomputer Information System Functional Design	55
	-2	ADAPSO Guidelines for Microcomputer Software Security	56
VII	-1	Strategies to Protect the Corporate Information Systems and Software Investment	60

U-SPR-I

I INTRODUCTION

A. BACKGROUND

- The magnitude of the computer security problem is just ~~surfacing~~ becoming apparent. A recent ~~report~~ investigation of the American Bar Association revealed that nearly 50% of 300 respondent companies reported losses of from two to ten million dollars ~~resulting~~ There losses resulted from:

  - Unauthorized computer use.
  - Theft of software.
  - Theft of assets.

- The survey showed that computer crime losses were predominately from within the organization.

- The executive felt that the gap between computer technology and security is widening.

- It is difficult to impress upon management that a magnetic tape (or micro disk) costing well under $100 contains information valued at over several million dollars.

- The objective of this Information Systems Program (ISP) report on Protecting the Corporate Software Investment is to evolve strategies of protecting software developed in-house and acquired from loss or unauthorized access in the mainframe, distributed, and personal computer environments.

- The subject chosen resulted from high client interest in rapidly changing information processing operating environment due to personal computers, and the growing importance of computer information security to corporate management.

- This report is targeted toward the information systems manager, the vice president of administration, and the corporate security director.

B. SCOPE AND METHODOLOGY

- Although this report includes a global discussion of information system security, its main focus is on software security, both applications and systems software developed in-house and acquired. The report considers software security with respect to utilization on host processors, the distributed environment, and personal computers.

- The report can be used as an aid in planning for software security in a rapidly changing information systems environment, including distributed processing and widespread use of personal computers.

- The research program consisted of interviewing both vendors (ten) and users (six), particularly users involved with security issues related to microcomputers. Additional material was gathered from interviews with industry experts, from INPUT's research file and from an extensive literature search and analysis.

- The research summary analysis and findings are organized in the following ~~chapters:~~ manner:

  - Chapter II is the executive summary in presentation format and a supporting discussion.

  - Chapter III covers the ~~people aspects~~ personnel issues related to protecting the corporate systems and software investment.

  - Chapter IV outlines the process of and options in developing a software security methodology.

  - Chapter V presents strategies for designing and developing secure systems and application software.

  - Chapter VI examines the implications of and emerging technology related to protecting corporate systems and software in the microcomputer and distributed processing environment.

  - Chapter VII summarizes and recommends ~~people~~ personnels, administrative, and technology strategies to protect the corporate systems and software investment in a rapidly changing information systems environment.

- Appendix A contains specialized definitions that relate to computer information system security.

- ~~A~~ Related INPUT reports ~~are~~ are contained in Appendix B.

- The vendors' questionnaire is found in Appendix C.

II EXECUTIVE SUMMARY

- Note: This executive summary is designed in a presentation format in order to:
  - Help the busy reader quickly review key research findings.
  - Provide ready-to-go executive presentations complete with a script, to facilitate group communication.
- The key points of the entire report are summarized in Exhibits II-1 through II-3. On the left-hand page facing each exhibit is a script explaining its contents.

A. ESTABLISH A BASELINE FOR INFORMATION SYSTEMS AND SOFTWARE PROTECTION

- The transfer of electronic intelligence from the data processing center to the user environment makes protecting information systems and software a people, and hence a top management, problem. It is essential that corporate management be aware of the awakening security giant and be involved in the strategies of protecting the corporate information nerve centers used to conduct the heart of corporate business activity.

- The key to coping with information systems dynamics is the careful selection of the security director, his placement high in the corporate organization, and backing by top management.

- Protecting the corporate system and software investment is in the final analysis the responsibility of well-motivated users at each corporate level. Education promoting awareness and responsibility best motivates personnel to maintain protection of corporate trade secrets, this information systems and software.

- Cost-effective ~~coating~~ of corporate information systems and software in ~~layers~~ with available and emerging security technologies in the mainframe, user network, and intelligent teminal areas can raise the ante of commiting fraud to prohibitively high or at least insurable level.

B. SECURITY PROTECTION IS A THREE-DIMENSIONAL ASSESSMENT

- Strategies for protecting the corporate information systems and software investment are assessed in three dimensions: (1) people really count; (2) good administration is a necessary component; (3) technology is the first line of defense.

- Strategies related to users at all levels include: (1) corporate security policy, promulgated and backed by top management, which incorporates user responsibilities, code of ethics, and risk assessment; (2) selection of a security director experienced in company operations, placed high in the corporate organization, backed by and responsible to top corporate management; (3) heightened user awareness through continued, varied, and ~~current~~ briefings to small groups of users and executives; and (4) personnel strategies ~~including~~ background investigation, hiring and termination procedures, annual security evaluations, and, as necessary, separation of duties.

- Basic administrative strategies include fire protection with preferably halon systems; duplicate storage of system applications software, preferably encrypted and at two outside secure locations; legal protection through copyright and trade-secret registration; and insurance under complying conditions against both fraud and disaster.

- Use of technology to protect corporate information systems and software as the first line of defense requires cost-effective selection of available and emerging technologies for (1) host processors including mainframes and distributed minis; (2) user networks including telecommunication and LANs; and (3) intelligent terminals including word processors and personal computers.

C. LAYERED TECHNOLOGY IS THE CORE DEFENSE

- Carefully selecting multiple and independent technologies available for host, including mainframe and distributed processors; user networks, including telecommunications and Local Area Networks (LANs); and intelligent terminals, including word processors and personal computers, is the first line of defense for protecting the corporate information systems and software investment.

- Security options available at host processors include operating system add-on security monitors; selectively available secure operating system kernels; applying formal structure design methodologies and structured programming to in-house and contractor-developed software; and the application of secure change control, including checking for clearing main and scratch pad memory, trap-doors, and trojan horses.

- Encryption, both private and public key; authentication, including user, host, and tap-proof fiber optic LANs; and multi-line telephone access controllers are technologies available to protect user networks at selected levels of cost/effective security.

- Protecting corporate information systems and software contained in intelligent terminals in the user environment represents the most rapidly growing area of vulnerability. Available technologies include secure microprocessors (Intel iAPX286), secure software microdisks (PROLOK), terminal identifiers, and microprocessor-encapsulated active (smart) plastic cards.

III

III PEOPLE, THE KEY TO ~~THE~~ SYSTEM AND SOFTWARE SECURITY

A. SECURITY, A TOP MANAGEMENT RESPONSIBILITY

- Of the 26 possible threats to corporate information systems as shown in Exhibit III-1, nearly 70% are countered by good operational practices, physical security, and personnel—all of which are the responsibility of top management.

III-1

- The Information Systems (IS) manager, chief of the vault where valuable electronic resources are stored, has responsibility for defending against ~~increasing~~ threats to the core of the corporate information system.

- Experience has shown that the major vulnerability is within the organization, often with trusted employees who know ~~both~~ how the company and the information system works.

- Top management involvement is a top priority requirement when establishing a baseline for information security. Corporate policy, a joint effort between the chief administrative office, the security director, and the IS director, should be promulgated by the chief executive officer. Policy with respect to personnel should include:

  - Organization policy, including ~~the~~ placement within the organization, ~~the~~ responsibilities, and ~~the~~ authority ~~of the security director.~~

- Hiring practices, including interview and thorough background checking for all personnel, ~~including~~ managers that are involved with developing and using corporate information systems and software, should not be excepted.

- Termination practices, including fixing for cause, security debriefing, and termination interviews.

- A Code of conduct, including security review, conflict of interest, non-disclosure, and sanctions.

o Development, communication, and implementation of corporate security policies is analyzed in ~~this~~ the following sections of this chapter.

B. A WELL-PLACED SECURITY DIRECTOR

o Each new generation of computer technology gives birth to new professional positions. The computer security expert has evolved along with third-generation technology (i.e., IBM 360, DEC VAX) sometime between 1968 and 1972. ~~The distribution of~~ computer power, ~~including~~ personal computers in the end-user environment, is rapidly ~~increasing~~ the importance of information system security ~~to corporate well-being.~~ Today, increasing, especially via, accelerating

o The functions of a well-administered security program are:

- Avoidance of loss through risk removal (such as background investigation prior to hiring).

- Deterrence of financial ~~toward~~ through ~~such things as~~ separation of duties and security briefings.

- Prevention, such as with use of physical access control devices (e.g., CARD-activated turnstiles and doors).

- Detection through the use of auditing.

- Recovery through disaster recovery services, insurance, and legal proceedings.

- Correction through security review and software change control procedures.

o A must for a successful corporate security program is the selection and strategic placement of a well-qualified information system security director.

o At the minimum the security director must report directly to the top IS executive, or more ideally to the corporate executive responsible for overall corporate security, (with a close interface to the IS director).

o Information security directors should have both an understanding of the information system and of the business in general. A senior information system analyst/programmer having prior experience in a major operating department is a preferred candidate.

o Managing information system security successfully requires experience in and understanding of the interplay among systems development, audit, users, senior management and information systems operations.

o The security director serves as liaison between senior management and the end users. However, the director's first loyalty is to senior management. Close working relationships with IS and Audit are essential.

o Information security should be the security director's sole responsibility. Information security, including disaster recovery, needs full-time attention.

- To be successful a security director must be supported by top corporate management.

C. PEOPLE SECURITY FACTORS

- Operating in an information environment where the number of users having access to corporate information is rapidly rising, personnel security factors are likely the most cost-effective alternative to controlling system and software security. The following factors are considered baseline with respect to reducing people-related risk to an operationally acceptable level:

1. BACKGROUND INVESTIGATION

- As a major method of avoidance, background investigations are worthwhile for new employees, contractor personnel, vendor personnel, consultants, and on a periodic basis for anyone in a position of trust.

- To avoid possible legal (or other, such as union) problems, authorization for background investigations should be obtained as part of the employment application or vendor contractual agreement.

- Background investigations are usually performed by an outside agency, such as Equifax. Equifax, a company specializing in insurance/credit investigation, interviews employers, co-workers, neighbors, and researches public records. Equifax charges $20-$100/person.

- Items for verification are education, prior work experience, criminal convictions (if any), opinions of qualified people who know the candidate, and employer performance reports.

- o Under most circumstances full disclosure of the findings to the prospective employee (with an opportunity for rebuttal) is recommended policy.

2. EMPLOYEE HIRING PROCEDURES

- o ~~Upon an employee's acceptance,~~ Before hiring an employee, an agreement of confidentiality, a patent agreement, and an acknowledgement of a professional code of conduct should be executed.

- o An initial briefing on security should be scheduled soon after the candidate is hired.

3. CORPORATE INFORMATION SECURITY POLICY

- o The corporate information security policy should establish goals, objectives, requirements, and responsibilities promulgated by the CEO.

- o A visible and enforceable information security policy indicates a top-to-bottom commitment to security and represents a primary form of security deterrence.

- o To be effective, security policy must be kept current.

4. EMPLOYEE EDUCATION

- o Perhaps no other factor has greater cost-effectiveness than small and frequent security briefings to all levels of the corporate organization. Typical of educational policies is that of Chevron Oil Company:

  - As part of its consciousness-raising effort, Chevron conducts a series of two-hour presentations and demonstrations that familiarize top managers with security issues ~~ranging from~~ Topics include personal computers, ~~through~~ time sharing, ~~to~~ and data base access, to mainframes.

- The seminars are presented to small groups of between six and eight executives.

5. SECURITY PERFORMANCE EVALUATION

o A security performance evaluation should be explicitly included as part of job performance and merit increase reviews. The review includes managers' assessment of employee support and of adherence to corporate security policies.

o Suggestions from employees and other interested parties should be solicited, reviewed with the security director, and acted upon.

6. CODE OF CONDUCT

o A code of conduct for all employees, contractors, and consultants covers rules of behavior to protect the organization from potential losses.

o A code of conduct should be explicit in describing sanctions that will be applied in response to code violations.

o The code should be reviewed periodically, such as at security briefings or at performance reviews.

o It is advisable to have employees (etc.) acknowledge the code by signing it.

o A typical code of conduct for information processing is shown in Exhibit III-2.

7. SEPARATION OF DUTIES

o Duties should be assigned ~~to employees in positions of trust~~ with security in mind. Duties should be separated to minimize the lone employee's ability to engage in criminal activity without detection.

- o There should be multiple control, whereby one person initiates the task, another verifies correctness, and a third is held accountable for the total task. This is a useful method where highly sensitive information is involved.

- o Job rotation is another means of stopping and uncovering ongoing fraud.

- o Mandatory vacation policies can be used to interrupt continuity and to expose ongoing fraud.

8. TERMINATION PROCEDURES

- o Termination for cause requires immediate removal of the employee from a position of trust.

- o Terminated employees should receive a debriefing with explicit explanation of ex-employee responsibilities, such as maintaining confidentiality of trade secret and other competitive information. A terminating agreement should be signed and executed.

- o A security director should ensure that material such as access cards and software documents are returned, and that necessary computer access passwords and secret keys are changed.

IV

IV ESTABLISHING A SOFTWARE SECURITY METHODOLOGY

A. SOFTWARE SECURITY ADMINISTRATION

1. SOFTWARE DESIGN AND DEVELOPMENT

- Security aspects for design and development of ~~secure~~ software are covered in detail in Chapter V, Designing for Secure Software.

2. DOCUMENTATION CONTROL

- Secure software administration requires that software documentation and control be established as the separate responsibility of a software librarian. The librarian is responsible for maintaining the software library in paper and magnetic form in source language, for logging copies in and out, and for duplicating software documentation in any form.

- It is essential that obsolete or duplicate text and other paper documentation of critical programs be shredded to avoid scavenging.

- Terminated employees should be required to check out with the software librarian for clearance as part of the termination procedure.

3. FIRE PROTECTION

- The software library is best protected from fire through the use of a halon fire control system. Because of its chemistry, halon poses the least threat to people, magnetic media, and paper.

4. DISASTER RECOVERY

- Software recovery procedures are a critical part of any disaster recovery plan. Two backup copies of the complete software library are required and should be stored ~~perferably~~ at separate locations. In the event of disaster, a backup set of the complete software will still exist while one set is being used to restart system operations.

- A further level of security can be obtained by encrypting the software library prior to transmission or delivery to off-site locations.

5. LEGAL

- Legal aspects of software protection include patents, copyrights, and "trade secrets."

- Establishing patent rights to software is extremely difficult. Copywriting a program, whether by ~~stationary~~ statutory or common law, offers a degree of protection that has in some notable instances been successfully enforced, but (particularly in the microprocessing software area) has been largely avoided.

- Viewed by many as the best alternative form of legal protection ~~is that given to~~ for "trade secrets," ~~through tort law.~~ Courts have applied a reasonably standard set of tests to determine the legality of trade secrets and whether the trade secret has been used in an unfair or improper way.

6. INSURANCE

- "A sleeping giant," ~~insurance~~ is expected to have a positive effect on the security problem. Insurance requirements ~~conditions for insurability~~ promote formalization and standardization of security methodologies and increase top management awareness of information system security at all organizational levels.

B. OPERATIONAL SOFTWARE SECURITY OPTIONS

- Each of the operational software security options shown in Exhibit IV-1 independently offers a level of security protection. The greatest level of security is obtained, as will be discussed below, by layering multiple options to make the cost of penetration prohibitive ~~to the prospective attacker~~.

1. PASSWORDS

- Passwords are perhaps the lowest form of security protection from unauthorized access or modification of corporate information software.

- Password capability is provided by virtually all operating systems.

- Passwords can be user created or (preferably) security system assigned. A secure means of mapping the user to the assigned password is essential.

- Encrypting the password resident in operating system tables adds a level of security without sacrificing operating efficiency.

- Passwords should be changed frequently and at irregular intervals.

- Passwords are easily determined by a determined hacker.

2. TERMINAL IDENTIFIER

- Selective terminals have the ability to be uniquely (a high probability) identifed as ~~an~~ input-output resources, either in the direct access or dial-in mode.

- Some terminals have the capability of ~~reaching~~ reading magnetic stripe cards containing user IDs to identify the user at a particular terminal as having the right to access or modify corporate information software.

- A password is an identifier (preferably ~~by~~ system generated and assigned) giving rights of access to system resources. A password is usually (but not necessarily) assigned to one use. A personal ID is a secret value that is known only to the user and separately supplied to the security monitor that uniquely identifies a user.

- Passwords, personal IDs, and terminal identifiers can be combined to add another level of operational software security.

3. SECURITY MONITORS

- Another dimension of operational software security can be obtained by using a security monitor on top of existing operating systems. Securing monitors are software packages that reduce the frequency of unauthorized access or improper use of corporate information system resources.

- Some of the more popular security software packages for IBM-compatible mainframes are shown in Exhibit IV-2. Security monitors differ in function, for example:

  - Alert and secure are targeted for protecting against unauthorized access from the interactive terminal or CICS environment.

IV-2

- ACF 2 and top secret offer great flexibility in discretionary access policy, whereas RCAF implements an inflexible and mandatory security policy.

- Only ACF2 and secure have versions compatible with the VM operating system.

- Top secret and alert are the only packages that do not require changes to the operating system upon installation.

o Security monitors require a security administrator to map the relationship between users and resources. The matrix is then stored (often encrypted) in a protected area of the security monitor.

o Security monitors attempt to solve deficiencies in operating systems that have not been designed with security in mind. As such, security monitors are vulnerable to a determined hacker.

o Discussion of the design of secure operating system software is presented in Chapter V, Designing for Secure Software.

o Advanced security monitors provide for the capability of implementing security policies that are discretionary, mandatory, or a combination of both.

- Discretionary policy allows a specific user or process to create objects (i.e., files) and then specify who has access to them.

- Mandatory security policy establishes a hierarchy of security classifications as a basis for determining access.

o Effective security monitors are easy to install (i.e., require few if any operating system modification), are efficient (i.e., low system overhead), are

on-line and flexible with respect to the security administrator, and are capable of mapping terminals and users to both system resources (i.e., processors and peripherals) and objects, including software, data bases, files, records, and data.

- Security can be increased by providing both software memory protection (i.e., insuring that processes are limited to a memory segment) and execution domains (a hierarchy of executable system processes). These functions are more efficiently implementable in hardware. (See Chapter VI, The Microcomputer and Software Security.)

- Security monitors vary, as shown in Exhibit IV-1, in their ability to interface with operating systems, protect local and dial-in data communication subsystems, control system software functions, and provide levels of password support.

- Security monitors are generally good at providing audit trails. Audit capability includes:

  - System access.

  - Access Attempts.

  - Resource use.

  - Security violations.

  - Interrelationship between users and resources.

  - On-line monitoring of suspected violators.

- Effective security monitors disconnect both unattended ~~intended~~ terminals (after a preselected or ~~from time to time~~ varied times) and users who make

repeated (i.e, more than two) unsuccessful attempts to access the system from the same terminal.

4. ENCRYPTION

- Encryption is an ~~holly~~ effective way to protect system and software from active intrusion.

- Encryption is particularly effective in cases of remote access, program transmission, downloading, program library, and outside program storage.

- There are currently some major drawbacks to the widespread use of encryption for commercial systems.

  - Encryption systems tend to be expensive.

  - Encryption tends to degrade system performance.

  - Secret key generation and distribution need careful administrative attention.

- Encryption can be accomplished through software products, through security modules including specialized micro chips, and through completely automated electronic systems that include key management.

- The most widely used single key encryption system uses as an algorithm, the Digital Encryption Standard (DES) promulgated by the National Bureau of Standards (NBS). The 64-bit key (56 data plus 8 parity bits) ensures that the current cost of key discovery is prohibitive.

- By using multiple encryption, master and subset key management systems ~~that~~ permit secure transfer through multilevel nodes within corporate information systems. A major problem is the complexity of key generation,

distribution, and management.

- Another method of public-key encryption utilizes two keys related by a one-way function. This method permits one key to be published to all interested parties. The key management problem is significantly reduced, but there are, at the present time, greatly increased computational requirements to encrypt the information for transmission, storage, etc. INPUT expects that within two years a effective electronic solution will be forthcoming.

5. TELEPHONE ACCESS CONTROLLERS

- Telephone access controllers interpose between remote dial-up terminals and the host computer dial access ports, as shown in Exhibit IV-3. The controllers do not wait for an unthorized user to gain computer access before enacting countermeasures. Access is denied to the computer if a user does not dial from a previously authorized location or does not enter the correct access code.

- Access controllers operate in an analog mode. The controller does not acknowledge that it is being accessed. The user keys in a valid location identification number (LIN). The access controller then answers with an acknowlegement tone or message and both the user and the unit disconnect.

- Within approximately 15-20 seconds the controller calls a preselected telephone number and interconnects the terminal at that number with the computer modem, permitting the user to initiate the sign-on procedure.

- Typical controllers handle 32-64 incoming lines, and include additional features, such as hard copy audit trail and time-dependent callback programming.

- Since the initial interface to the dial-up terminal is analog, the telephone access controllers are relatively secure from external attack.

- o Some controllers track and audit each remote interconnection from terminal modem to computer modem, thus ensuring that a valid sign-on has been accomplished.

- o Most controllers have the ability to handle ~~both~~ up to four simultaneous calls and queuing of 28 others.

- o It is possible to use a telephone access controller in conjunction with the encryption equipment shown in Exhibit IV-2 to provide an even higher level of computer software security. Telephone access controllers are usually programmmed through a dedicated terminal. Some can also be programmed through a remote terminal, where the remote terminal is protected from unauthorized access by a single access controller having a preprogrammed callback procedure.

6. SMART CARDS

- o A smart card consists of a plastic card in which is embedded a customized chip comprising:

  - A microprocessor with interfaces for memories and communication with the outside world.

  - Scratch pad memory (random access).

  - A program memory (read only).

  - A "user memory" (programmable read-only memory).

- o There is no internal power source. The micro processor is passive until the card is inserted into a terminal.

- The user memory is under exclusive control of the micro-program in the read-only memory. During the last stage of manufacturing process the user memory is divided into areas with different rights of access as shown in Exhibit IV-4.

- After initialization the contents of the secret area cannot be accessed externally. Information stored in the secret area is accessible for internal use only. The secret area is used to store authentication codes of the card issuer, a personal card holder identification code, and encryption keys.

- Access to the confidential area is protected by the secret codes of the card issuer and the card holder.

- No restrictions exist in accessing the open memory.

- The user will insert the card in the terminal and enter the password (personal identification number), which will be stored in encrypted form in the confidential memory. If one utilizes a one-way algorithm (involving keys stored in the secret memory and the user's identification number) and transmits the result encrypted between the terminal and the host system, it can be determined that:

  - The card is valid.

  - The user is properly identified (with high probability).

  - The user is connected to a valid host processor.

- A further level of security can be achieved by adding an electronic signature consisting of a sequence number (including a date-time group) in the transmitted information, thus encrypting the information utilizing the secret authentication key.

- The technology makes falsification very difficult. Fraud requires an advanced chip manufacturing facility, and possession of proprietary information from the chip manufacturer, the card manufacturer, and the card issuer.

7. OTHER TECHNOLOGY

- The other technology under development promises to tie user identification to unchanging personal characteristics. Technologies ~~which~~ that strengthen the identification process are:

  - Fingerprints: matching stored information with active finger impressions using holography.

  - Hand Geometry: matching stored information about palm lines using holography.

  - Signatures: matching stored digitized patterns of signatures with dynamic analysis of handwriting.

  - Voice prints: matching digitized information with digitized speech sound waves ~~of active speaking.~~

- These technologies have been reviewed in the INPUT report shown in Appendix B. ~~Related INPUT Reports.~~

- Although promising, none of the above technologies is yet sufficiently reliable or economically viable.

V

V DESIGNING FOR SECURE SOFTWARE

A. SYSTEMS SOFTWARE

1. OPERATING SYSTEMS, THE KEY TO INFORMATION SECURITY

- To date, the best approach for designing secure operating systems is the security kernel concept.

- A smaller, less complex, and more easily verifiable security module is possible by separating the security-relevent functions of the operating system into a kernel.

- The security kernel is a reference monitor that checks the legality of every reference between user (subject) and resource (object). Included are programs, files, terminals, printers, etc.

- The security kernel mediates every access to protected resources. By isolating the security kernel from the rest of the operating system, the module can be more effectively protected from users and system programmers.

- The greatest difficulty has been in verifying that security kernels operate and that they implement security policy correctly.

- Security kernels implement discretionary or mandatory (or a combination of both) security policies. Discretionary policy allows the user or security officer to specify objects and who has access to them. As shown in Exhibit V-1, discretionary policy is implemented as either a security matrix or as an access/control list that is related to each protected object. Accounting personnel can only read information in File B, whereas user 3 (department head) can either read from or write into File B.

- As implemented by the security officer, mandatory security policy establishes several classifications (such as "secret" or "confidential") of the user's level of clearance and of the resources (object). Security may further subdivide categories of both on the basis of "need to know."

- Memory protection (that is, preventing one process from changing another) is an architectural key for system software security. The efficiency of memory protection (and of a secure operating system) is directly related to hardware features that permit dividing a virtual memory into segments that are accessible through discriptors. As shown in Exhibit V-2, another layer of information system security is provided through the implementation of "execution domains" in software, hardware, or firmware. Again, secure system performance is highly dependent on hardware features, with three domains essential for efficient operation.

  - The most privileged is the security kern
    security mechanism.

  - Software such as user identification, auth
    auditing (that is) closely related to the sec
    verified and if possible proven and correct
    either its own domain or, in a three-domain
    operating-system domain.

Software (such as for user identification, authentication, and security auditing) is closely related to the security kernel; is carefully verified and if possible proven correct.

This software runs either in its own domain or, in a three-domain system, in the operating-system domain.

- Execution domains restrict the access of programs in

to a few well-defined interfaces with more privileged domains.

- The security monitors shown in Exhibit IV-2 provide discretionary security as an add-on feature to IBM mainframe operating systems. Secure operating system implementations on most current mainframe architectures have proved too inefficient for commercial use. Supporting by both memory protection and executive domain hardware, the SCOMP operating system, running on Honeywell's level 6/DPS6 system, is perhaps an exception.

- Secure versions of UNIX implemented on minicomputers and microprocessors are expected within the next year. (See Chapter VI, The Microcomputer Software Security, for discussion of the Intel iAPX286).

2. DATA BASE MANAGEMENT SYSTEMS, A PROBLEM AREA

- Data base management systems (DBMSs) allow many people to have access to different types of data, most frequently in a "user friendly" manner. Whereas security monitors with operating systems control access to the file and record (program) level, DBMS systems can add information system security down to the data level.

- The data base administrator (security officer) to defines access and use of all but local user data.

- Two approaches to security access are utilized by DBMSs: explicit and constrained. In explicit systems only defined user/data set relationships are effective; users can have access to all other resources.

- In constrain systems, unless the data base administrator authorizes an individual (program) to perform an operation, no one but the administrator (super user) can access or manipulate the information. Care must be taken with constrained systems such that security does not become a bottleneck to efficient DBMS use.

- o Access to DMBS resources may be enforced through either a set of flexible authorization rules or through more formal data classification schemes. Authorization rules that control user access can be:
  - User specific.
  - Time specific.
  - Logical subsets of rows or columns.
  - Specific DBMS operations.
- o Query languages (powerful tools for retrieving, appending, replacing, deleting, and aggregating DBMS information) are frequently used for defining and enforcing authorization rules. For example and as shown in Exhibit V-3, the query system arbitrates each request, filtering through such portions as are authorized for access and response, thereby denying the user knowledge of protected information.
- o Although some constraints (such as references to single records) are possible, security with respect to statistical data bases remains a significant problem. Clever computer hackers can successfully extract valuable information (programs) through successive queries that form and valid authorizations.
- o The basic objective of security with respect to DBMSs is the achievement of a high level of security without compromising system performance or user friendliness.

B. APPLICATIONS SOFTWARE

- o Development of secure application software uses most of the software engineering practices related to a formal design methodology and structured programming.

1. DESIGN

- o Development of secure application software depends on establishing clear interfaces between functions (modules) and minimizing information transfer from module to module.

- o A structured design utilizing a top-down hierarchical approach is a favored design methodology.

- o Data typing that relates data to its related processes (called "data abstraction") allows definition of small, self-contained modules. Establishing the module's interface allows the concept of encapsulation (i.e., black box) or "information hiding" to be used to control access. Additional function can be added to the module without affecting its security features.

- o The design should carefully establish the least privilege access to modules, programs, and application to later control program access and change.

- o The auditing process must be considered as integral to the design process.

2. PROGRAMMING

- o Structured programming techniques (where each module has one entry point, all paths within the module are active, and one exist point) greatly increase the probability of successful verification and increased security.

- o A level of security can be achieved by assigning portions of large programs to separate programmers.

- When the program is completed those modules related to control should be separated from procedures so that following validation the entire program, or at least control modules, can be encrypted.

3. VALIDATION

- Validation should be accomplished by a separate group.

- The validation process should ensure that all paths of each module are active and that any "trapdoors" used for debugging during development are removed.

- Unusual ranges and combinations of input data are useful for uncovering results not specified as output.

- Checks should be made that the program erases scratch pad memory and auxiliary storage as the last process before termination.

- The above techniques reduce the probability of "trojan horse" attacks whereby ~~a temporary change with insertion of instructions is made, which, under select~~ inserts temporary instructions and someone that, under select conditions, executes during production time, breaching software or data security.

- The validation process should ensure that audit trails are operational and effective.

4. MAINTENANCE

- All changes to operational programs should go through formal change control procedures, whereby changes are made at regular intervals, are done on a controller basis, and are properly reviewed.

- Periodically the production program should be compared with the master to ensure that the production copy exactly matches.

- Both software that translates known object code back to source (decompilers) or assembly (disassemblers) language and the flow charting of utility programs all help to maintain application software security by ensuring that the object code

do not contain trapdoors or trojan horses.

VI

VI THE MICROCOMPUTER AND SOFTWARE SECURITY

- Intelligent terminals (in the form of workstations, word processors, and personal computers) (both standalone and in local area networks,) add a whole new dimension to the problem of corporate information system and software security.

- Technological information processing innovations ~~addition~~ may well be outpacing technical solutions to the corporate security problem. In the final analysis, security strategies with respect to people may form the major bulwark in protecting the corporate investment in information systems, and software.

A. MANAGEMENT

- It is clear that management must establish a policy with respect to the procurement of, responsibility for, and use of office automation equipment before the problem gets out of hand. Limiting the type and variety of equipment and storage media is certainly in order.

- A vigorous education program (including frequent small classes, briefings, and risk assessments) ~~and~~ that is ~~targeted~~ designed to heighten awareness is likely the most cost-effective strategy for maintaining security in the microcomputer/office automation environment.

- As more corporate strategic information is developed on magnetic media in the user environment, management will be forced to give greater attention to security issues, for example:

  - Acquisition strategies (that have been developed in draft form on word processors and then routed through LAN's to executives), could theoretically be intercepted by anyone with access to the LAN.

  - Corporate investment strategies that were reproduced by the chief financial officer's executive secretary and now reside on a personal computer flexible disk can be used by anyone with a compatible system.

- Management must implement a strategy by which the individual user carries primary responsibility for that portion of the corporate information system (including hardware, software, and data) that is under the user's direct control.

- Alternatively, management must provide users with appropriate technical safeguards as outline below.

B. DISTRIBUTED PROCESSING

- Distributed processing offers managers and staff the ability to use local computer power to better meet their individual processing needs. Although hardware and software support problems increase security complexity, distributed processing does offer several advantages:

  - Software and data can be isolated to a specific functional area (i.e., personnel, accounts receivable, etc.).

- People in that area know each other and can easily recognize intruders.

o Distributed systems require great attention to the information flow within (LANs) and between distributed processing nodes. Technologies exist, and are becoming increasingly and more economically available, to respond to both active and passive intrusion into the distributed processing network.

1. ENCRYPTION

o Where encryption is used, it is usually important that the information passing through nodes (between source and destination) be protected from unauthorized access via a node.

- Public key encryption systems can easily be applied to distributed processing but, at the present time, only with a significant loss in system efficiency. Where transmission volume is small (i.e., downloading software), a public key system can be highly effective.

- Private key systems (i.e., DES) can be applied to distributed systems utilizing master/multiple-key management systems utilizing multiple encryption methodologies.

2. SIGNATURES

o In a distributed network it is often necessary to identify not only the source (user) but also the receiver (host, node, etc.). The receiver should be identified as well to ensure that the information transmitted is valid and came from the identified source.

- Authenticators (which are one-way functions of secret information keys), one key known only to the user and the other key known only to the host) establish trusted (with high probability) interconnections.

- An information transmission identifier (sequence number, date, and time group) that is properly authenticated ensures (with high probability) that the information transmission is from the identified user.

3. FIBER OPTICS

o The fiber optic medium is almost impossible to tap into. As such, fiber optics are an ideal candidate for LANs and for other networking applications.

- Fiber optics are becoming attractive for new buildings under construction.

- Several Bell Operating Companies (BOC's) are developing fiber optic telecommunication circuits.

o Fiber optics will become the prefered medium of transmission ~~(preference~~ particularly for LANs) by the end of the decade.

C. SYSTEM AND SOFTWARE SECURITY

1. PHYSICAL

o Personal computers and word processors are tempting targets for theft. They are even more attractive than typewriters.

o Depending on corporate policy, micro workstations can be secured through:

- Anchor-pads.

- Lockable power switches.

- Lockable equipment enclosures.

o Lockable space should be provided to users for storage of flexible disks. In a sensitive area selected disks can be under the control of a designated librarian with responsibility for ensuring that they are logged in and out to the appropriate personnel.

2. ACCESS CONTROL

o Early personal computer, word processing, and office workstation systems were targeted for single-user, single-program, and standalone use. As such, little need was seen for security access control.

o The current generation of microprocessors provides for multifunction and on-line operating environments. Technical solutions to security access problems are just beginning to appear.

o Vendors are offering firmware in the form of an intelligent programmable circuit board extension to IBM PC-compatible and other-vendor PCs. The firmware provides access restriction through passwords, encryption methods for data and software protection, audit trail of computer usage, and methods for either local or central security control.

3. SECURE MICROPROCESSOR

o Secure operating systems have long been held as the key to system and software security. All operating system functions related to system security have been incorporated in what is called a security "kernel". (See Chapter V, Designing For Secure Software.)

- Support for multiple processors.

- Control over a large, segmented ~~of~~ virtual memory.

- A minimum of three execution domains.

- Control of access to input/output devices.

o The concept of a secure microprocessor information system is shown in Exhibit VI-1. The ideal processor has four execution domains, the most privileged being level zero. ~~The domains in effect prevent~~ lower domains are prevented from executing system functions in higher domains.

VI-1

o Intel Corporation has developed the iAPX286 chip with the architectural feature outline above, which reduce by a factor of eight the overhead in implementing a secure information system.

o INPUT expects that a secure UNIX microprocessor operating system utilizing the Intel microprocessor will begin appearing in intelligent terminals within the next two years.

4. SECURE DISK STORAGE

o In an effort to ~~achieve~~ deterrence of software piracy, the Association of Data Processing Service Organizations (ADAPSO) established the technical guidelines shown in Exhibit VI-2.

VI-2

o The most successful solution today appears to come from the Vault Corporation with its prolok disk. The process places a special hardware-like "fingerprint" on a currently conventional 5-1/4-inch, double-density, double-sided diskette. In addition to the identifier, the disk contains a 10,000-byte administrative and encoding program encrypted by the same process used to protect the software that the user (vendor) later loads.

- The program loaded onto the disk has been encrypted and an additional 3,000 bytes that tie the program to the fingerprint encryption process have been added.

- Neither the program nor the operating system require modification.

- The encrypted program can be loaded onto a hard disk, but operating the program requires the presence of the prolok flexible disk to decrypt the program resident on the hard disk.

- An advanced product under development will permit the program to be shared (as authorized) among users in an LAN.

- A hardware technique under development modifies utilized vendor disk drives to create software diskettes that place marginal-strength pulses in selective locations in a program.

  - Personal computers are able to read the weak pulses and execute the program, but the pulses are too weak to permit copying onto another disk.

  - The technique can be used to control the number of times a program is used before it becomes inoperable.

VII

VII SUMMARY

- A combination of strategies involving motivating people and selectively using technology are necessary to protect the corporate software and systems investment.

- A flexible approach to security in an information system environment ~~that~~ is characterized by rapid technological change and increasing user involvement is the optimal overall strategy to pursue.

- This study has shown that no one single or indeed no small group of strategies can ensure adequate protection to corporate information, including software.

- The principle of layering or putting up a number of independent (hopefully, simultaneous) roadblocks that make penetration very time consuming and costly ~~is probably~~ the most important ~~of a number of strategies~~ strategy to pursue. is

- The dimension of the strategy ~~that forms the tripod to~~ protect the corporate investment in information systems and software, people, administration, and technology are shown in Exhibit VII-1.

A. PEOPLE COUNT

- Involvement of top management is a must in order for corporate information systems and software security to be effective.

- Selection and placement of a security director (backed by management) is critical to security planning, implementation, and administration.

- In the final analysis the corporate information system and software investment is protected by the user (people). Multiple strategies are necessary to heighten people's awareness of and commitment to protecting corporate information:

  - Background investigation prior to hiring in order to increase the probability of employee trustworthiness.

  - New employee acknowledgement of security responsibility upon hiring.

  - Definitive corporate information security policy promulgated by top management and kept current.

  - A program of employee education to small groups and at frequent intervals.

  - Security performance evaluation as part of the annual and merit review process, with employee reacknowledgement of security responsibilities.

  - Publication of a corporate code of conduct that has clear sanctions for abuse.

  - Separation of sensitive duties among employees to minimize individual fraud and make collusion very difficult.

- Security debriefing and acknowledgement of postemployment responsibilities with repect to corporate information, as part of termination procedures.

B. ADMINISTRATION NECESSARY

- There are a number of administrative strategies available that primarily relate to the physical security of corporate information systems and software.
- A software librarian ensures the authorized possession, distribution, and documentation control of corporate software.
- An adequate fire protection system (preferably halon) affords a high degree of systems and software survivability.
- A strategy of storing two copies of the corporate information system and application software (encrypted) in separate locations assures disaster recovery.
- Corporate information system applications software can be protected through copyright and trade secret law.
- Insurance is becoming a more popular strategy for giving additional protection to the corporate software investment.

C. TECHNOLOGY, THE CORE DEFENSE

- The importance of security has spawned a number of technology options, some still emerging, which are at best struggling to keep pace with technogical innovation in distributed processing, LAN, and micro-driven office automation intelligent terminals.

- Some security monitors are more successful than others and add on to already-inefficient existing operating systems. These monitors emulate security kernels, and provide a satisfactory degree of mediation between subjects (users) and objects (resources).

- Telephone access controllers are the most recent addition to mediating access between users and hosts in rapidly expanding remote telecommunications (primarily dial-up) networks.

- Microprocessor-encapsulated "smart" cards promise to add another layer of validation for the user and to add authentication for interconnections and transmissions between users and processors.

- Encryption (software and hardware) is on a rapidly decreasing cost curve. Private and eventually public-key-driven, encryption is becoming a viable strategy for secure transmission and authentication of information between and at distributed processing nodes.

- Fiber optics, particularly for new construction, offers highly cost-effective security, particulary for LANs.

- A number of products are becoming available or already exist to protect the corporate system and software investment as microprocessors proliferate among corporate users. The two most promising appear to be the prolock secure disk storage, which prevents access to and duplication of vendor-

puchased or in-house-developed system and applications software, and the Intel 16-bit iAPX286 microprocessor, which incorporates hardware security features and should soon permit the development of an efficient UNIX security kernel for standalone and LAN computing environments.

- Many strategies are available for designing security into system and application software. Placing all security-related functions in an operating system kernel, providing memory protection by segmenting virtual memory, implementing privileged execution domains, and mediating access through a reference monitor are all strategies for developing secure coporate information operating systems.

- Security strategies for development and application software include: formal structured design methodology; structured programming; data abstraction including information hiding; separated and formal validation to uncover trapdoors and possible Trojan horse attacks; and maintenance procedures including formal change controls; periodic matching of production programs to the master library copy; and utilization of software aids that permit decompilation, disassembly, and testing for dead code, unspecified or unusual output, or cleared scratch pad memory and auxiliary storage.

APPA

APPENDIX A: DEFINITIONS

- Access: The ability to use a resource.
- Access Control: Granting a suitably authorized request for access to information system resources.
- Attack: An attempt to effect unauthorized access.
- Audit: Use of a log in determining whether access is controlled in accordance with management policy and generally accepted accounting practices.
- Authenticate: To determine the accuracy of a user's identity or a message's certification of its time or place of origin.
- Authorize: To permit the use of a sensitive resource.
- Browse: Unauthorized reading of data in the hope of attaining useful information whose specific location is not known by the browser.
- Category: An aggregation of sensitive resources formed to facilitate authorization.
- Class: A level of authorization applied to a set of users. These users may read all data whose class is equal to or less than their own.

- Create: Develop and associate a resource with an identifier.
- Destroy: Cause a resource to cease to exist.
- Diddle: To write (data) with an intent to confuse or deceive.
- Disconnect: To deny access to the system resulting from repeated attempts to have a user's claim of identity authenticated.
- Discretionary security: Asssignment of rules to specify who is allowed what type of access to which objects. Discretionary security allows those who own a segment of data to decide who can have access to it.
- Encryption: A process for protecting program and data that must be stored on or transmitted over media that cannot be otherwise protected against unauthorized monitoring.
- Cryptography: a form of access control applicable to sensitive resources that are beyond the scope of program access control and physical access control.
- Exhaustion: An attack carried out by entering all possible values (for example, of a password) and trying to supply a secret quantity unknown to the hacker.
- Group: A set of users selected to facilitate authorization.
- Hacker: An individual, usually outside a corporate organization, who attempts to gain unauthorized access to the corporate information system through random or systematic attacks.
- Identifier: a value uniquely associated with a user, a group of users, or a sensitive resource.

- Individual-based Authorization: Permitting or denying access to users according to previously recorded individual authorization, with that interaction accompanying a request for access (individualed ~~as contrast to~~ rather than resource based).

- Interval: The maximum length of time that a user may use a particular value (such as a password) as data for authentication.

- Kernel: A security kernel is a hardware/software mechanism that contains all security-relevent operating system functions. Implementations may contain one component, called the kernel, which enforces a specified set of security rules. Other components are called trusted processes.

- Last-used: The time log when a particular user most recently made use of the system.

- List: A set of authorizations that are applied to one resource or to a set of resources.

- Log: Data recorded about authorizations and requests for access.

- Mandatory security: The enforcement of a security policy that uses a fixed security classification such as top secret, secret, etc. to determine access.

- Masquerade: Someone posing as another; a mechanism used in an attack.

- Password: Data a user provides for purposes of authentication.

- Penetration: An unauthorized access that gives the hacker control of the system; a type of attack.

- Physical data: Anything other than magnetically recorded data to which the system can control access; concerns portable media in computer centers and libraries.

- Program: Magnetically recorded data to which the system can control access.

- Protocol: A procedure for communicating between two or more nodes of a network.

- Query: A request for information from a data base; specifically one for data collected from a number of records, and presented as a sum, average, etc.

- Read: To acquire data.

- Reduce: To process logs so as to extract only the data needed for auditing purposes.

- Reference Monitor: A computer system component that checks each reference from subject (users or program) to object (file, device, user, or program) determine if the access is valid.

- Request: An application for the right to affect access to sensitive resources.

- Residual: Data left after a process is completed; undestroyed residual data is subject to attack by a browser.

- Resource: Any service, capacity, device, or data accessible by a system.

- Resource-based: Permitting or denying access to users according to their ability to provide authenticating data and association with a resource request.

- Salami: An attack involving many small amounts, for example a misappropriation of very small sums.

- Sensitive: A resource of sufficient value such that access control is desired.

- Scavenge: Conduct an attack by browsing through discarded printed material.
- Sign: Appended to a collection of data, authenticating data indicative of the sender, place, time, origin, etc.
- System Integrity: The extent to which a system resists penetration.
- Ticket: An authorization that is associated with a user for a specific time or limited number of accesses.
- Time Bomb: A routine that for the programmer's own purposes executes an attack after a set time.
- Time Stamp: Authenticating data indicative of the time that an event took place (for example, the sending of a message).
- TOCTTOU (time of check to time of use): Failing to protect data between the time that the system validates its data and the time that the system uses the data, thus permitting penetration.
- Tracker: A query or set of queries designed to make it possible for a user to set data base information without proper authorization.
- Trap-door: An exit or hook that permits easy access to a system or new code to be easily added to a program; a mechanism used in an attack.
- Trojan Horse: A routine that does not contribute to the documented function of the program that contains it, but instead is something the program's developer would prevent if possible (a routine that takes advantage of the program's security level to effect unauthorized access).
- Trusted: A component that can be relied on to enforce the relevant security policy.

- Use: Access to a resource for the purposes for reading, writing, creating, or destroying it.

- Write: To modify data.

- Zap: An unauthorized modification of a program that the user does not have authorization to use.

App B

APPENDIX B: RELATED INPUT REPORTS

- o New Issues In Computer Security, December 1982.

App. C

Vendor Questionnaire

U-SPR

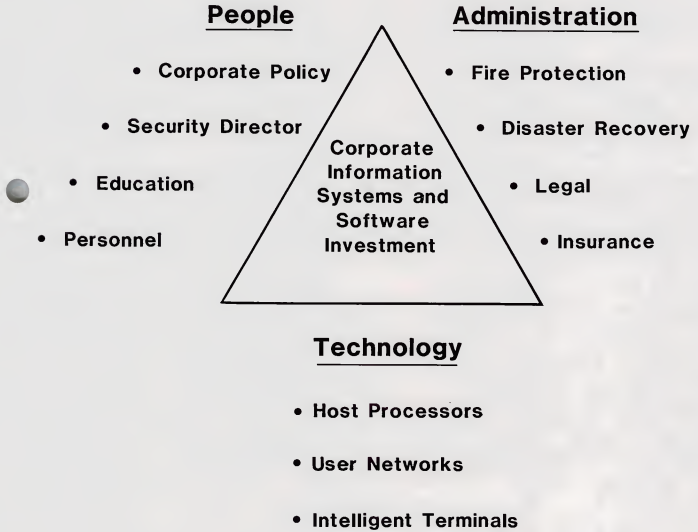
ESTABLISH A BASELINE FOR INFORMATION SYSTEMS AND SOFTWARE PROTECTION

- Involve Top Management
- Carefully Select and Place Security Director
- Motivate Users to be Responsible
- Use Multiple Physical Protection Strategies
- Layer Technology as the Core Defense

© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT II-2

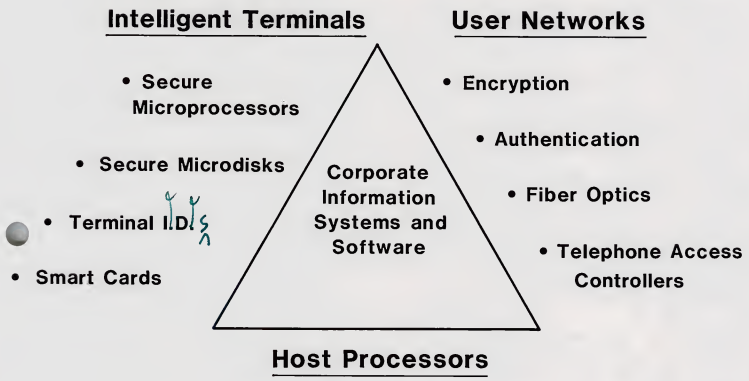
SECURITY PROTECTION IS A THREE-DIMENSIONAL ASSESSMENT



© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT II-3

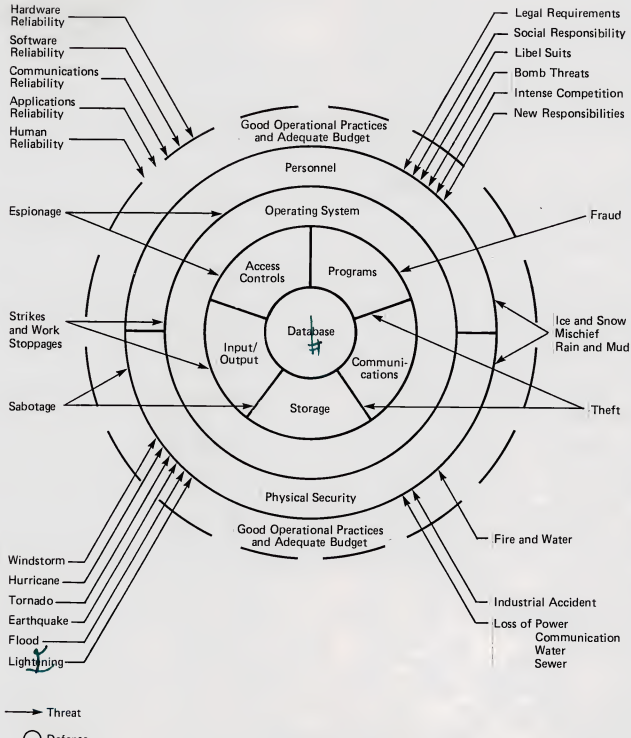
LAYERED TECHNOLOGY IS THE CORE DEFENSE



© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT III-1

DEFENSE AGAINST POSSIBLE THREATS TO
CORPORATE INFORMATION SYSTEMS



© 1984 by INPUT. Reproduction Prohibited.

USR

EXHIBIT III-2

INFORMATION SYSTEMS CODE OF CONDUCT

The information systems department is entrusted with computer programs, supplies, data, documentation, and facilities that are continuously growing in size and value. We must maintain visible standards of performance, security, and conduct that aid in our efforts to assure the integrity and protection of these assets. The following policy should be used in conducting on-the-job activities. The success of this program, however, requires that each member of the information systems organization maintain an awareness of the value of the information with which he or she has been entrusted. Violation of this trust is grounds for disciplinary action, including immediate dismissal. IS must:

- Conduct all activities to preclude any form of dishonesty, such as theft or misappropriation of money, equipment, supplies, documentation, computer programs, or computer time.
- Avoid any act that compromises ~~one's~~ integrity, such as falsification of records and documents or unauthorized modification of production programs and files. Refuse gratuities from vendors, agencies, or other resources.
- Avoid any act that may create a dangerous situation, such as carrying a concealed weapon on organization premises; assaulting another individual; or disregarding property, safety, and security standards.
- ~~Do~~ not use intoxicating liquors, narcotics, or drugs while at work. ~~Do not~~ report to work while under the influence of same, or in any other way report in a condition unfit for work.
- Maintain courteous and professional relations with users, associates, and supervisors. Perform job assignments as requested by supervision or management and do so within the standards of performance and security. Report any observed violations of conduct or security as soon as possible.
- Adhere to the no-solicitation rule, and all other employment policies.
- Protect the confidentiality of sensitive information with regard to competitive positions, trade secrets, or assets.
- Exercise sound business practice in the management of company resources, such as personnel, computer usage, outside services, travel, and entertainment.

Employees must not

© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT IV-1

LEVELS OF SECURITY

LEVEL	OPTION	ADVANTAGES	DISADVANTAGES
1	Passwords	Low Cost	Most Vulnerable
2	Terminal IDs	Low Cost	Inflexible
3	Security Monitors	Good Security Audit Trail	High Cost Needs Administration Susceptible to Systems Programmers
4	Encryption	High Security	Major Cost Degrade System Performance Needs Administration
5	Telephone Access Controllers	Good Internal Security High External Security Good Audit Trails Analog System	Internal Security Susceptible to Systems Programmers
6	Smart Cards	Very High Security Authentification of Both User and Host Flexible	Currently High Cost Needs Administration

© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT IV-2

LEADING SECURITY MONITORS FOR

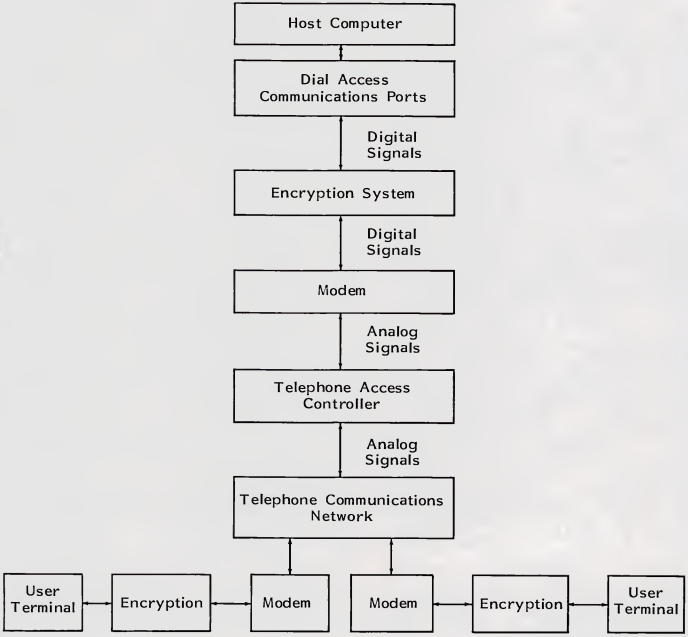
IBM PLUG-COMPATIBLE SYSTEMS

FUNCTION	ITEM	SECURITY MONITOR					
		SAC	Alert/ CICS	RCAF	ACF2	Secure/ CICS	Top Secret
Compatible with Operating Systems	MVS	●	●	●	●	●	●
	VSI	●	●		●	●	
	OS/MVT		●			●	
	DOS/VSE	●	●				
	SVS					●	
	VM				●		●
I/O and Data Systems Protected	TSO	●	●	●	●	●	●
	IMS	●		●	●		●
	CICS	●	●	●	●	●	●
	Roscoe	●			●		●
Functions Controlled	JES/JCL/SCAN	●			●		
	Allocate	●	●	●	●		●
	Scratch	●	●	●	●	●	●
	Open	●	●	●	●	●	●
	EOV	●	●	●	●	●	●
	Catalog	●	●	●	●		●
	Recatalog	●	●	●	●		●
	Uncatalog	●	●	●	●		●
	Rename	●	●	●	●	●	●
Password Support	Inserts Password on Submit				●		●
	Changes Passwords	●	●	●	●		●
	Forces Password Change at Established Intervals		●	●	●		●
	Logs Password History		●	●			●
	Warns of Password Expiration		●	●	●		●

© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT IV-3

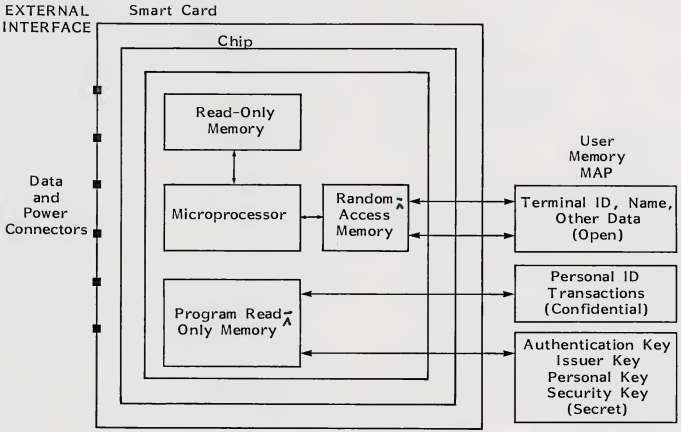
TELEPHONE ACCESS CONTROLLER
SECURITY SYSTEM INTERFACE



© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT IV-4

SMART CARD FUNCTIONAL DESIGN

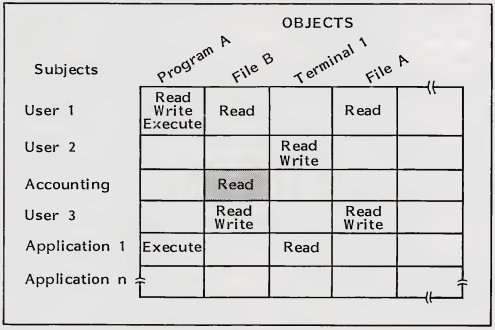


© 1984 by INPUT. Reproduction Prohibited.

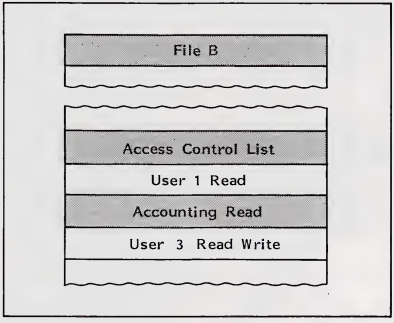
EXHIBIT V-1

IMPLEMENTATION OF DISCRETIONARY SECURITY POLICY

MATRIX CONTROL



LIST CONTROL

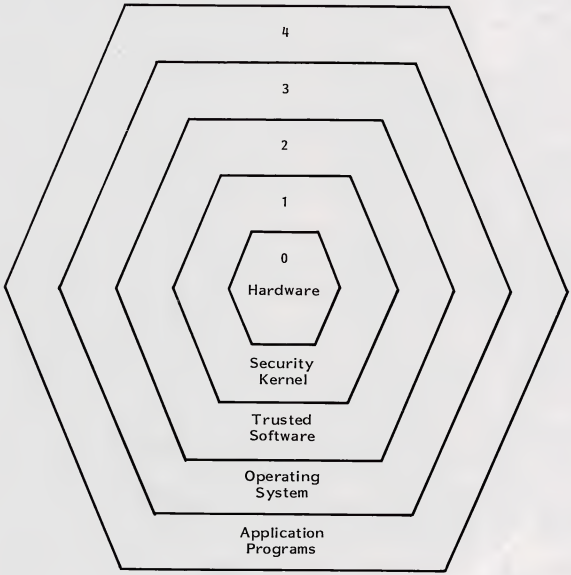


= Discussed in Text

© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT V-2

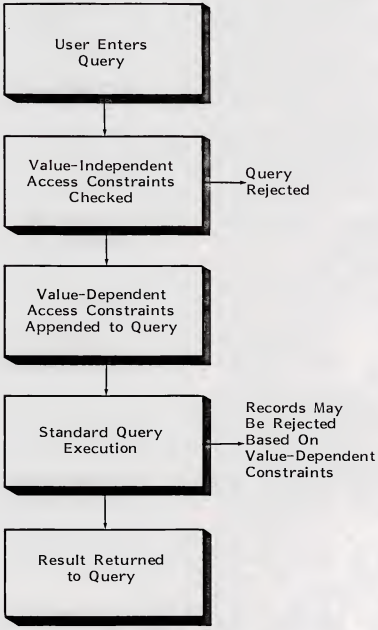
SECURE INFORMATION SYSTEMS EXECUTION DOMAINS



© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT V-3

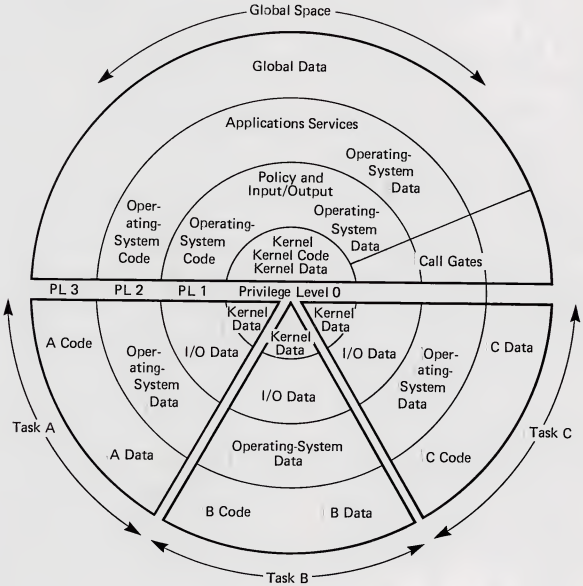
ARBITRATION OF USER QUERIES
TO PROTECT DBMS RESOURCES



© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT VI-1

SECURE MICROCOMPUTER INFORMATION SYSTEM FUNCTIONAL DESIGN



© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT VI-2

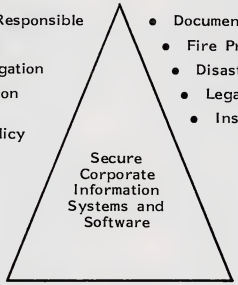
ADAPSO GUIDELINES FOR MICROCOMPUTER SOFTWARE SECURITY

ITEM	GUIDELINES
Cost	• Low to end user • Cost to install is small part of total system manufacturing cost
Ease of Use	• Ease of installation • Transparent to end user • No effect on program execution, speed or performance • No complex rules or keys to remember • User can make backup copies
Installation	• Simple for manufacturers to install
Availability	• Widely available to all software publishers • Can be used with all types of software requirements
Hardware Requirements	• Can be used on all floppy disk sizes and formats • Minimal use of RAM • Can be used on hard disk • Used on wide variety of microcomputers • Transferal to other computers • Can be transferred with computer to new owner
Operating System Requirements	• Used on wide variety of operating systems • Does not interfere with operating system • No new definitions to operating systems
Protection	• Provides security from duplication by end user • Protects software from external duplication

© 1984 by INPUT. Reproduction Prohibited.

EXHIBIT VII-1

STRATEGIES TO PROTECT THE
CORPORATE INFORMATION SYSTEMS AND SOFTWARE INVESTMENT



PEOPLE COUNT

- Top Management Responsible
- Security Director
- Background Investigation
- Hiring and Termination Procedures
- Corporate Security Policy
- Education
- Personal Security Evaluations
- Code of Conduct
- Separation of Duties

ADMINISTRATION NECESSARY

- Documentation Control
- Fire Protection
- Disaster Recovery
- Legal
- Insurance

TECHNOLOGY, THE CORE DEFENSE

- Passwords and Terminal IDs
- Security Monitors
- Telephone Access Controllers
- Smart Cards
- Encryption
- Fiber Optics
- Secure Microprocessors
- Secure Microdisk Storage
- Security Operating System Kernels
- Formal Design Methodologies
- Structured Programming
- Change Control

© 1984 by INPUT. Reproduction Prohibited.

APPENDIX C

CONFIDENTIAL

INPUT QUESTIONNAIRE

CATALOG. NO U S P R
SIC. CODE
SIZE CODE
AREA CODE
STUDY CODE
DATE MM DD YY

STUDY TITLE:
TYPE OF INTERVIEW: ☒ VENDOR ☐ USER ☐ TELEPHONE ☐ ON-SITE ☐ MAIL

INTERVIEWER: _____

COMPANY: _____ CO. TYPE: _____

ADDRESS: _____ SALES: _____

_____ # EMPL: _____

CITY: _____

STATE: _____ ZIP: _____

INDUSTRY ☐

☐ DISCRETE MANUFACTURING
☐ PROCESS MANUFACTURING
☐ TRANSPORTATION
☐ MEDICAL
☐ SERVICES
☐ UTILITIES
☐ RETAIL
☐ BANKING
☐ WHOLESALE
☐ OTHER
☐ INSURANCE
☐ GOVERNMENT- FEDERAL
☐ GOVERNMENT-STATE & LOCAL
☐ EDUCATION

INTERVIEWS

NAME TITLE TELEPHONE NO.

SUMMARY

REFERENCES

CATALOG NO. USPR

PROTECTING THE CORPORATE SOFTWARE INVESTMENT
VENDOR QUESTIONNAIRE

1. What products/services do you offer related to program/data security?

	Product Name	Number of Users	Price Range
1.			
2.			
3.			
4.			

2. What mainframe/mini operating systems do you support?

	IBM	Burroughs	Honeywell	DEC	HP	Others
Mainframe/ Minis						
Operating Systems						

3. What are the levels of program/data security that your products provide?

- ☐ Personal _____
- ☐ Terminal _____
- ☐ Program _____
- ☐ File _____
- ☐ Data _____
- _____ _____
- _____ _____

4. How are audit trails provided?

_____

_____

_____

_____

5. How does the product provide for:

Multi-CPU Environment/Site

Multisite Environment

Distributed Environment

6. To what extent does the product/system provide for protecting the program/data by encryption?

☐ None ☐ DES ☐ Other

7. What modifications are necessary to incorporate the product into the operating system environment?

☐ None

☐

8. What is the overhead associated with the use of your product?

☐ System Efficiency: _____

_____

☐ User Access: _____

_____

9. What products do you offer in relation to program/data security for personal computers?

☐ None

	☐ IBM/PC (Compatible)	☐ Apple	☐ DEC	☐ Others
Product Name	_____	_____	_____	_____
Operating System	_____	_____	_____	_____
Users	_____	_____	_____	_____
Price Range	_____	_____	_____	_____

10. How is program/data security accomplished for personal computers?

☐ Hardware _____

_____

☐ Software _____

_____

☐ Disc _____

_____

☐ _____ _____

_____

11. Who (up to 3) are your major competitors?

		Mainframe/Mini	Micro
Vendor	1.		
	2.		
	3.		

12. What are the trends you see in providing program/data security?

☐ Hardware _____

_____

☐ Software _____

_____

☐ Market _____

_____

_____ _____

_____